

A Proof Checking View of Parameterized Complexity

Luke Mathieson

Abstract

The PCP Theorem is one of the most stunning results in computational complexity theory, a culmination of a series of results regarding proof checking it exposes some deep structure of computational problems. As a surprising side-effect, it also gives strong non-approximability results. In this paper we initiate the study of proof checking within the scope of Parameterized Complexity. In particular we adapt and extend the PCP[$n \log \log n$, $n \log \log n$] result of Feige *et al.* to several parameterized classes, and discuss some corollaries.

1 Introduction

The straight-forward view of most computational complexity classes is one of what problems can be solved given certain computing power and resource restrictions. Alongside this is the *verification* view of complexity, where we ask not what can be computed within a given set of restrictions, but whether a given solution can be verified under certain restrictions. The most famous of these is of course the equivalent definitions of NP as the class of all problems that can be solved in nondeterministic polynomial time or verified in deterministic polynomial time. This definition may be thought of as a *proof system*, where a Turing Machine (the verifier) has access to the input and a proof, and in polynomial time checks that the proof is correct.

With access to a random bit string, it is possible to reduce the number of bits that the verifier reads from the proof. In fact, in the case of NP , this is quite a surprising reduction; with only a logarithmic number of random bits, we need only a *constant* number of bits from the proof to verify the proof. The trade-off being that if the proof is false, we may incorrectly accept it, but with probability at most one half.

Such proof systems have been well studied for traditional complexity classes such as NP , $PSPACE$ and $NEXP$. In this paper we begin to look at parameterized complexity through the same lens. In particular we demonstrate a relatively simple but non-trivial proof system for $W[1]$. We also extend this to $W[2]$, $M[1]$, the bounded classes $EW[1]$, $EXPW[1]$ & $S[1]$ and the classes of the A -hierarchy up to $AW[*]$.

1.1 Useful History

This idea of classifying languages by membership proofs began to attract serious attention in the early to mid eighties, with Goldwasser, Micali & Rackoff's [24] introduction of the idea of *interactive proofs* (later published in a more complete form [25]) and Babai's [5, 9] *Arthur-Merlin games*. Both probabilistic approaches to proof verification.

Over time these classes were linked back to traditionally defined complexity classes. The class of problems with interactive proofs is precisely PSPACE [30]. The class of problems with Arthur-Merlin style verifiers that use a polynomial number of rounds turns out to be the same as the class of problems with interactive proofs [26]. If multiple, non-communicating provers (defined in [10]) are allowed we obtain NEXP [7, 8] (Ben-Or *et al.* [10] also showed that for any number of provers, there was an equivalent protocol with at most two provers).

This work culminated in the development of *probabilistically checkable proofs* [3] and what is now known as the PCP Theorem:

Theorem 1 (The PCP Theorem [2, 4]). *NP is the class of all languages that can be verified by a polynomial-time probabilistic Turing Machine (the verifier) that can access at most $O(\log n)$ random bits and at most $O(1)$ bits of an oracle string (the proof) such that any input that is in the language is accepted with probability 1 and any input that is not in the language is accepted with probability at most $\frac{1}{2}$.*

Dinur [17] gives more accessible proof, via constraint satisfaction.

Far from being a theoretical curiosity, PCPs have a number of applications across computer assisted mathematics [6] and cryptology [25] but possibly most interestingly PCP results have implications for approximation algorithms. It is PCP results that led to inapproximability results for MAX-WORD [16], MAX-3SAT [2], MAX-CLIQUE [20] and in general that if $P \neq NP$ then no MAXSNP-hard problem is in PTAS.

2 Parameterized Complexity Theory

A *parameterized problem* is a decision problem augmented with a special input, the *parameter*. This may be more formally viewed as a language over some alphabet with a *parameterization* that provides a positive integer parameter for each instance.

Definition 2 (Parameterized Problem). *A parameterized problem over alphabet Σ is a pair (Π, κ) where $\Pi \subseteq \Sigma^*$ and $\kappa : \Sigma^* \rightarrow \mathbb{N}$ is a parameterization.*

Typically given an instance, the parameterization (as a function) is implied and we treat inputs as being accompanied by a integer, usually denoted k .

Parameterization allows a more relaxed notion of tractability:

Definition 3 (Fixed-parameter Tractability). *A parameterized problem (Π, κ) is fixed-parameter tractable if there is an algorithm \mathcal{A} and a computable function f such that for all inputs $(x, \kappa(x))$ the algorithm \mathcal{A} decides if $x \in \Pi$ in time bounded by $f(\kappa(x)) \cdot |x|^{O(1)}$. The class of all fixed-parameter tractable problems is FPT.*

This then gives a natural reduction schema:

Definition 4 (FPT Reductions). *Given two parameterized problems (Π_1, κ_1) over Σ_1 and (Π_2, κ_2) over Σ_2 , an fpt reduction from (Π_1, κ_1) to (Π_2, κ_2) is a mapping $R : \Sigma_1^* \rightarrow \Sigma_2^*$ such that for all $x \in \Sigma_1^*$:*

1. $x \in \Pi_1 \Leftrightarrow R(x) \in \Pi_2$.
2. R can be computed in time bounded by $f(\kappa_1(x)) \cdot |x|^{O(1)}$.
3. There is a computable function g such that $\kappa_2(R(x)) \leq g(\kappa_1(x))$.

The last condition results in a very rich intractability theory for parameterized complexity. We will give details of the classes relevant for this paper, but a much fuller treatment can be found in the monographs of Downey & Fellows [19] and Flum & Grohe [22].

We first define a hierarchy of propositional logic formulæ. Let $\{a_i\}$ be a set of boolean literals, then we define the following formula classes:

$$\begin{aligned}\Gamma_{0,d} &:= \{a_1 \wedge \dots \wedge a_c \mid c \leq d\} \\ \Delta_{0,d} &:= \{a_1 \vee \dots \vee a_c \mid c \leq d\}\end{aligned}$$

These can then be recursively stacked to give the classes $\Gamma_{t,d}$ and $\Delta_{t,d}$:

$$\begin{aligned}\Gamma_{t,d} &:= \left\{ \bigwedge_{i \in I} \phi_i \mid \phi_i \in \Delta_{t-1,d} \right\} \\ \Delta_{t,d} &:= \left\{ \bigvee_{i \in I} \phi_i \mid \phi_i \in \Gamma_{t-1,d} \right\}\end{aligned}$$

In addition we denote by Φ^+ the subclass of a class of propositional formulæ Φ where no literals are negated and by Φ^- the subclass of Φ where all literals are negated. Given a propositional formula over a variable set X a truth assignment that sets k variables of X to TRUE is called a *weight k assignment*¹ or an assignment of weight k .

¹This use of “weight” is standard in the parameterized complexity literature, but may conflict with definitions from other areas. In this paper, when we refer to the weight of an assignment, this is the meaning we intend.

The fundamental problem for many parameterized intractability classes is the WEIGHTED SATISFIABILITY problem:

WSAT(Φ)

Instance: A boolean formula $\phi \in \Phi$ and a positive integer k .

Parameter: k .

Question: Is there a satisfying assignment for ϕ of weight k ?

We can then define the W -hierarchy:

$$W[t] = [\text{WSAT}(\Gamma_{t,d})]^{FPT}$$

where $t + d > 2$ and $[X]^{FPT}$ denotes the closure of a parameterized problem X under fpt reductions.

Even though we do not have quite the latitude to reduce the structure of the formula as in classical complexity (where everything in NP can be reduced to a formula in 3-CNF), we can impose slightly more restriction to the formulæ. In particular:

$$W[1] = [\text{WSAT}(\Gamma_{1,2}^-)]^{FPT}$$

and

$$W[2] = [\text{WSAT}(\Gamma_{2,1}^+)]^{FPT}$$

So for every problem in $W[1]$ we can convert any instance into an instance of the WEIGHTED SATISFIABILITY problem where the formula is in 2-CNF and all literals are negated and for every problem in $W[2]$ we can convert any instance into a CNF formula (of unbounded clause length) where all literals are positive (similar statements can be made for the other classes in the W -hierarchy, *q.v.* [22]).

At the other end of the parameterized intractability scale is the direct definitional analog of NP:

Definition 5 (*para-NP*). *A parameterized problem (Π, κ) is in para-NP if there is a computable function f and nondeterministic Turing Machine that on input $(x, \kappa(x))$ decides $x \in \Pi$ in time bounded by $f(\kappa(x)) \cdot |x|^{O(1)}$.*

It turns out however that *para-NP*-complete problems seem much harder than $W[1]$ -complete problems and that $W[1]$ provides a more natural analog of NP^2 .

The class XP provides an alternate perspective on parameterized intractability:

²Very loosely speaking, barring a collapse, *para-NP*-complete problems correspond to problems with time complexity $(\kappa(x))^{|x|}$ or worse, whereas $W[1]$ -complete problems have complexity $|x|^{\kappa(x)}$ (this bound is more formal than the given *para-NP* one as the W -hierarchy is contained in XP [22].)

Definition 6. A parameterized problem (Π, κ) is in XP if there exists a computable function f such that every instance $(x, \kappa(x))$ is decidable in time

$$|x|^{f(\kappa(x))} + f(\kappa(x))$$

The entirety of the W -hierarchy is contained in $\text{para-NP} \cap \text{XP}$.

XP in a certain sense plays a role similar to a parameterized version of EXPTIME, and as such contains a hierarchy that bears a relationship to the polynomial hierarchy and PSPACE, the A -hierarchy.

Similar to the polynomial hierarchy, the A -hierarchy can be characterized by alternating quantified satisfiability problems. In this case of course, there is a parameterized flavour:

$\text{AWSAT}_l(\Phi)$

Instance: A boolean propositional formula $\phi \in \Phi$, with the variable set X partitioned into l sets X_1, \dots, X_l and positive integers k_1, \dots, k_l .

Parameter: $k = \sum_{i \in [l]} k_i$.

Question: Is there a k_1 -sized subset of X_1 such that for all k_2 -sized sets of X_2 there exists a k_3 -sized subset of X_3 ... (&c. for l alternations) such that setting those variables to true satisfies ϕ ?

If we employ the notation \forall_k and \exists_k to denote “for all k -sized subsets” and “there exists a k -sized subset” respectively, we can reframe the slightly awkward definition of AWSAT_l by asking if

$$\exists_{k_1} X_1 \forall_{k_2} X_2 \dots Q_{k_l} X_l \phi$$

is true, where $Q \in \{\forall, \exists\}$. If we remove the bound on l , then we obtain the AWSAT problem, which has the same essential structure. When talking about this family of problems informally, we will omit the subscript and refer to them generally as AWSAT problems. These classes then provide the basis for the A -hierarchy:

$$A[l] = \begin{cases} [\text{AWSAT}_l(\Gamma_{1,2}^-)]^{FPT} & \text{for } l \text{ odd} \\ [\text{AWSAT}_l(\Delta_{1,2}^+)]^{FPT} & \text{for } l \text{ even} \end{cases}$$

One interesting superclass of the A -hierarchy is $AW[*]$:

$$AW[*] = [\text{AWSAT}(\Gamma_{1,2}^-)]^{FPT}$$

Thus $AW[*]$ is not entirely dissimilar to PSPACE^3 , however in the parameterized setting, there is no single analog of PSPACE, with its role being spread between $AW[*]$, $AW[\text{SAT}]$, $AW[P]$, XL and para-PSPACE [22].

³Or something between PSPACE and PH, though this also imprecise as natural parameterized versions of some PSPACE-complete problems are $AW[*]$ -complete. Conversely $\text{AWSAT}(\text{PROP})$, the parameterized alternating satisfiability problem for the class of all propositional formulae, is $AW[\text{SAT}]$ -complete and $AW[*] \subseteq AW[\text{SAT}]$.

2.1 Bounded Parameterized Complexity Classes

In the definition of FPT the function f that gives the dependence on the parameter is only restricted to being computable. We can define analogs of FPT and its intractability hierarchies with stronger restrictions on F that still retain very similar structures.

Definition 7 (EXPT). *A parameterized problem (Π, κ) is in EXPT if there is an algorithm \mathcal{A} and such that for all inputs $(x, \kappa(x))$ the algorithm \mathcal{A} decides if $x \in \Pi$ in time bounded by $2^{\kappa(x)^{O(1)}} \cdot |x|^{O(1)}$.*

Definition 8 (EPT). *A parameterized problem (Π, κ) is in EPT if there is an algorithm \mathcal{A} and such that for all inputs $(x, \kappa(x))$ the algorithm \mathcal{A} decides if $x \in \Pi$ in time bounded by $2^{O(\kappa(x))} \cdot |x|^{O(1)}$.*

Definition 9 (SUBEPT). *A parameterized problem (Π, κ) is in SUBEPT if there is an algorithm \mathcal{A} and such that for all inputs $(x, \kappa(x))$ the algorithm \mathcal{A} decides if $x \in \Pi$ in time bounded by $2^{o^{eff}(\kappa(x))} \cdot |x|^{O(1)}$.*

Typically the parameterizations of problems in SUBEPT are of a different character to normal parameterizations. In the subexponential theory the parameterizations play the role of “size measures” for the problem, rather than being independent of the size of the problem. Such measures may be for example the number of variables in a logic sentence or the number of edges and vertices in a graph (this is also in contrast to the length of the *encoding* of the problem).

These classes are accompanied by analogs of fpt reductions. These reduction schemes have slight technical differences to fpt reductions (*q.v.* [31], [23] and [27], or [22] for a collected survey of these and other related work), however they still produce hierarchies akin to the W -hierarchy, for $t \geq 2$:

$$EXPW[t] = [\text{WSAT}(\Gamma_{t,1})]^{EXPT}$$

$$EW[t] = [\text{WSAT}(\Gamma_{t,1})]^{EPT}$$

Although the first levels of these hierarchies are more technically delicate than the W -hierarchy, we still have the following key identities:

$$EXPW[1] = [\text{WSAT}(\Gamma_{1,2}^-)]^{EXPT}$$

and

$$EW[1] = [\text{WSAT}(\Gamma_{1,2}^-)]^{EPT}$$

⁴ $f \in o^{eff}(g)$ if there exists a computable, nondecreasing, unbounded function $h : \mathbb{N} \rightarrow \mathbb{N}$ such that $f(k) \leq \frac{g(k)}{h(k)}$.

The hierarchy corresponding to SUBEPT is mildly different⁵:

$$S[t] = \bigcup_{d \geq 1} [\text{SAT}(\Gamma_{t,d})]^{serf}$$

However we fortunately we also have that:

$$S[1] = [s\text{-var-WSAT}(\Gamma_{1,2})]^{serf}$$

Where *s-var-WSAT* is a different parameterization of the weighted satisfiability problem:

s-var-WSAT(Φ)

Instance: A formula $\phi \in \Phi$, an integer k .

Parameter: $\text{var}(\phi)$ (the number of variables in ϕ).

Question: Does ϕ have a satisfying assignment where k variables are set to TRUE?

2.2 The Miniaturization Isomorphism and the *M*-Hierarchy

The *S*-hierarchy, despite being a bounded hierarchy of parameterized classes, reflects structure in the unbounded theory. This structure can be elucidated via the *miniaturization isomorphism*. Given a parameterized problem (Π, κ) over Σ^* the *miniaturization* of the problem is

MINI- (Π, κ)

Instance: $x \in \Sigma^*$, and $m \in \mathbb{N}$ in unary such that $|x| \leq m$.

Parameter: $\lceil \frac{\kappa(x)}{\log m} \rceil$.

Question: Decide whether $x \in \Pi$.

Under this mapping we have the following:

$$(\Pi, \kappa) \in \text{SUBEPT} \Leftrightarrow \text{MINI}-(\Pi, \kappa) \in \text{FPT}$$

Consequently we can define an intractability hierarchy via this relationship, the *M*-hierarchy. For the purposes of this paper we need only the following:

$$(\Pi, \kappa) \in S[t]\text{-complete} \Leftrightarrow \text{MINI}-(\Pi, \kappa) \in M[t]\text{-complete}$$

However the *M*-hierarchy is closed under normal fpt reductions. The proofs of these results, and much more technical detail can be found in [22], or the original papers [1, 12, 14, 15, 13, 18, 21], for context however, it is known that for all $t \geq 1$ we have $M[t] \subseteq W[t] \subseteq M[t+1]$.

⁵Incidentally SUBEPT and the *S*-hierarchy correspond to parameterizations of the Exponential Time Hypothesis, making them particularly interesting parameterized classes. In fact, the entire *S*-hierarchy is contained in EPT, with EPT and SUBEPT bearing a similar relationship as XP and FPT.

3 Proof Checking, Interactive Proofs and PCPs

3.1 Notation and Notes

For convenience we denote by \mathbb{B} the set $\{0, 1\}$.

The proof systems will often be phrased somewhat like interactive proofs, as this often seems an intuitive, natural presentation, however the proof string is in effect a table of polynomial coefficients indexed by length m vectors over a field \mathcal{F} , along with the values of a truth assignment at points over this space.

3.2 Basic Definitions

Definition 10 (PCP). *A Probabilistically Checkable Proof System (a PCP) for a problem Π over alphabet Σ is a probabilistic polynomial-time Turing Machine V that given input x and access to a proof string $\sigma \in \Sigma^*$ satisfies the following conditions:*

1. *If x is a YES-instance of Π , there is a σ such that V^σ accepts x with probability 1.*
2. *If x is a NO-instance of Π , for every σ the probability that V^σ accepts x is at most $\frac{1}{2}$.*

The choice of 1 and $\frac{1}{2}$ as the probabilities for the completeness and soundness of the verifier are in a sense somewhat arbitrary, for example, Babai, Fortnow & Lund [7] use probabilities that vary with the length of the input, however the majority of results are stated directly with these probabilities, or are otherwise compatible.

Definition 11 (Restricted PCP). *Given two functions $r, p : \mathbb{N} \rightarrow \mathbb{N}$, a PCP is (r, p) -restricted if for every input x , V uses at most $O(r(|x|))$ random bits and $O(p(|x|))$ bits of the proof string σ .*

The set of all problems with a (r, p) -restricted PCP is typically denoted $\text{PCP}[r, p]$. With this notation we can thus succinctly restate Theorem 1:

Theorem 12 (PCP Theorem [2, 4]). $\text{NP} = \text{PCP}[\log n, 1]$.

3.3 Arithmetization Protocols

Lund *et al.* [28] introduced a protocol for demonstrating PCP and interactive proof results which they used to show that every problem in $\text{P}^{\#P}$ has an interactive proof (a key step in motivating Shamir's [30] result).

This protocol has proven to be extremely useful and has been used in whole or part for many of the PCP related results [2, 4, 7, 20, 30]. It is worthwhile to sketch an outline of this protocol to give an intuition for the working of the main result of this paper.

Given a complexity class \mathcal{C} we select a suitable \mathcal{C} -complete problem Π and produce a verifier that completes the following tasks:

1. For input x , the verifier constructs an arithmetical representation ϕ of x such that the value of ϕ is dependent on whether x is a YES-instance of Π or not. For example we may construct an arithmetic formula from a boolean formula such that the arithmetic formula is non-zero if and only if the boolean formula is satisfiable.
2. A sufficiently large field over which to do the arithmetic is chosen. Typically this will be \mathbb{Z}_p for some sufficiently large prime p .
3. The verifier then checks the arithmetical representation a variable at a time by instantiating a single variable and obtaining a simplified representation in one variable from the proof which it can use to compare against the expected value. If the simplified representation is satisfactory, the verifier picks a random value from the field, permanently sets the variable to this value and replaces the expected value by the evaluation of the simplified expression with that random value.
4. Step 3 is repeated until some value does not match expectation, at which point the proof is rejected, or until all variables have been instantiated at which point the expression is checked explicitly using elements of the solution obtained from the proof (*e.g.* values from a truth assignment).

The key to the effectiveness of this protocol is in the restriction on the arithmetic representation and the size of the field. For clarity of discussion we will assume the representation to be a multinomial and the field to be \mathbb{Z}_p for a sufficiently large prime p .

If the multinomial is of constant degree d , and the polynomial simplification over one variable obtained from the proof is false, it can agree with the true polynomial in at most d places [29]. So if the proof is false, it can “look true” for only a small number of values (d), and eventually some iteration of checking will observe an erroneous value with high probability ($1 - \frac{d}{p}$ where r is the number of iterations).

4 Parameterized PCPs

Clearly we can adapt PCP notions to parameterized complexity.

Definition 13 (Parameterized PCP). *A Parameterized Probabilistically Checkable Proof System (parameterized PCP, or p-PCP) for parameterized problem Π over alphabet Σ is a probabilistic FPT-time Turing Machine V that given input (x, k) , an instance of Π , and access to a proof string $\sigma \in \Sigma^*$ satisfies the following conditions:*

1. If (x, k) is a YES-instance of Π , there is a σ such that V^σ accepts (x, k) with probability 1.
2. If (x, k) is a NO-instance of Π , for any choice of σ the probability that V^σ accepts (x, k) is no greater than $\frac{1}{2}$.

As with non-parameterized PCPs, the completeness and soundness probabilities need not be 1 and $\frac{1}{2}$, however these values are sufficient for our purposes and confusing the notation thus serves no purpose.

Definition 14 (Restricted p -PCP). *Given two functions $r, p : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ a p -PCP is (r, p) -restricted if for every input (x, k) it uses $O(r(|x|, k))$ random bits and at most $O(p(|x|, k))$ bits of the proof string σ .*

We denote the set of all problems with an (r, p) -restricted p -PCP by p -PCP $[r, p]$.

For certain extreme values of the parameters, we can use the p -PCP $[r, p]$ notation to express some of the parameterized classes.

- $FPT = p\text{-PCP}[0, 0]$, by definition problems in FPT have no access to a proof and need no randomness.
- $FPT = p\text{-PCP}[f(k) + \log n, 0]$. An FPT -time algorithm can try all possible $f(k) + \log n$ random strings.
- $FPT = p\text{-PCP}[0, f(k) + \log n]$. An FPT -time algorithm can generate all proofs of length $f(k) + \log n$.
- $para\text{-NP} = p\text{-PCP}[0, f(k)n^{O(1)}]$. By definition.

4.1 A Non-trivial Parameterized PCP for $W[1]$

Theorem 15. *Let (ϕ, k) be an instance of $WSAT(2\text{-CNF}^-)$ where $\max\{\text{var}(\phi), \text{cl}(\phi)\} \leq 2^m$. There is an $(m \log m, m \log m)$ -restricted probabilistic FPT -time Turing Machine that rejects (ϕ, k) with high probability if (ϕ, k) is a NO-instance of $WSAT(2\text{-CNF}^-)$. That is, $WSAT(2\text{-CNF}^-) \in p\text{-PCP}[m \log m, m \log m]$.*

Proof. The protocol will follow the same general format as those of Lund *et al.* [28], Babai, Fortnow & Lund [7] and particularly Feige *et al.* [20] in that we will construct an arithmetic representation of ϕ and use the proof to evaluate this function pointwise.

Let ϕ be a 2-CNF^- with smallest m such that $2^m \geq \{\text{var}(\phi), \text{cl}(\phi)\}$. Denote each clause and variable by a binary string over m bits.

For $v \in \mathbb{B}^m$ and $i \in \{1, 2\}$ define a set of functions $C_{c,i} : \mathbb{B}^m \rightarrow \mathbb{B}$ as

$$C_{c,i}(v) = \begin{cases} 1 & \text{if } v \text{ is the } i^{\text{th}} \text{ variable of clause } c \\ 0 & \text{otherwise} \end{cases}$$

This can be done in such a fashion that each $C_{c,i}$ is multilinear in m variables. We sketch an example; say that $v = v_1 v_2 v_3 = 101$ is the 1st variable of clause c , then $C_{c,1} = v_1(1 - v_2)v_3$. Then the only place (over \mathbb{B}^3) where this is 1 is at 101.

Let $A : \mathbb{B}^m \rightarrow \mathbb{B}$ be a truth assignment to the variables of ϕ .

We then define the following function over some sufficiently large field.

$$SC(A, y) = \sum_{x_1, x_2 \in \mathbb{B}^m} \prod_{i \in \{1, 2\}} C_{y,i}(x_i) A(x_i)$$

This evaluates to 0 if and only if A is a satisfying assignment for clause y . Then ϕ in its entirety, can be expressed as:

$$S(A) = \sum_{z \in \mathbb{B}^m} SC(A, z) \cdot \prod_{i \in [1, m]} r_r^{z_i}$$

Where z_i is the i^{th} bit of the binary representation of z and (r_1, \dots, r_m) is a set of independently chosen random numbers from \mathcal{F} . This additional term is included to ensure with high probability that in the extended function the sum is zero only when all clauses evaluate to zero under A (again, Feige *et al.* [20] demonstrate the correctness of this method). However we must also verify that:

$$\sum_{z \in \mathbb{B}^m} A(z) = k$$

The first function now evaluates to zero if and only if all the clauses are satisfied and the second evaluates to k if and only if the weight of the truth assignment is k .

We now employ the following proposition:

Proposition 16 ([7], [20]). *Given a field \mathcal{F} , every boolean function f has a unique multilinear extension over \mathcal{F} . Moreover the value the extension at any point can be computed in time $2^{\text{arity}(f)}$.*

In particular we can compute the multilinear extension of C in any field of our choosing. Then assuming that A is close to multilinear, S is a multinomial of constant degree. Of course we cannot simply compute A in FPT -time, otherwise we'd have no reason for a p -PCP! However Babai, Fortnow & Lund [7] demonstrate a procedure for testing multilinearity of a function that fails with high probability if the function is not multilinear and succeeds otherwise. Feige *et al.* [20] improve this test, reducing the number of random and proof bits required to $O(m \log m)$.

We may now apply a protocol in the style of Lund *et al.* [28], though Feige *et al.*'s [20] version of the protocol is the direct inspiration.

Given a multinomial h of constant degree d over q variables the function $g_i(x_i)$ where the first $i - 1$ variables are randomly instantiated

$$g_i(x_i) = \sum_{x_{i+1}, \dots, x_q \in \mathbb{B}} h(r_1, \dots, r_{i-1}, x_i, \dots, x_q)$$

is a polynomial of degree d .

Assuming A is multilinear with high probability (to ensure the degree bound of the multinomial), given an expected value a_{i-1} we perform the i^{th} iteration of the proof check as follows:

1. Obtain from the proof the d coefficients of the polynomial g'_i that is purported to be g_i .
2. Check that $g'_i(0) + g'_i(1) = a_{i-1}$, if not, then reject.
3. If the first check passes, we may still have $g_i \neq g'_i$. However they can agree at at most d points in \mathcal{F} . We can check this with high probability $(1 - \frac{d}{|\mathcal{F}|})$ by randomly picking a value r_i , setting $a_i := g'_i(r_i)$ and verifying the formula recursively.

Initially we have $a_0 = 0$. The process continues until all variables have been randomly instantiated, at which point we can check the final function directly by obtaining the two values of A at the randomly generated points described by the instantiated variables and computing the value. By choosing \mathcal{F} such that $|\mathcal{F}| > \frac{md}{\varepsilon}$, the probability of accepting at some point over the m rounds is ε .

The function checking the weight of the satisfying assignment can be checked using the same protocol.

As $\log |\mathcal{F}| \in O(\log m)$, this protocol uses $O(m \log m)$ proof bits to obtain the polynomial coefficients and $O(m \log m)$ random bits in instantiating the function.

□

Corollary 17. *For every parameterized problem $\Pi \in W[1]$ there exists a function $f : \mathbb{N} \rightarrow \mathbb{N}$ such that $\Pi \in p\text{-PCP}[(f(k) + \log n) \log(f(k) + \log n), (f(k) + \log n) \log(f(k) + \log n)]$ and hence $W[1] \subseteq p\text{-PCP}[(f(k) + \log n) \log(f(k) + \log n), (f(k) + \log n) \log(f(k) + \log n)]$ where n is the size of the instance and k is the parameter.*

Proof. As $\text{WSAT}(2\text{-CNF}^-)$ is $W[1]$ -complete, every problem in $W[1]$ can be reduced to an instance of $\text{WSAT}(2\text{-CNF}^-)$ in time bounded by $f(k)n^{O(1)}$ for some computable function f . Hence the instance of $\text{WSAT}(2\text{-CNF}^-)$ produced by the reduced has at most $f(k)n^{O(1)}$ variables and $f(k)n^{O(1)}$ clauses. □

4.2 Unbounded Clauses and $W[2]$

The class $\Gamma_{2,1}^+$ of propositional formulæ can be more naturally thought of as the class of all propositional CNF formulæ. The protocol given for $W[1]$ in the previous section, although defined for $\Gamma_{1,2}^-$, does not depend on the clause length — the bounds on the number of bits used may change, but

the clause length is not fundamental to the structure, unlike say, that the formula is in CNF as this restriction ensures that the arithmetization is multilinear.

Theorem 18. *Let (ϕ, k) be an instance of $\text{WSAT}(\Gamma_{2,1}^+)$ where $\max\{\text{var}(\phi), \text{cl}(\phi)\} \leq 2^m$ and p is the length of the longest clause. There is an $(p \cdot m \log m, p \cdot m \log m)$ -restricted probabilistic FPT-time Turing Machine that rejects (ϕ, k) with high probability if (ϕ, k) is a NO-instance of $\text{WSAT}(\Gamma_{2,1}^+)$. That is, $\text{WSAT}(\Gamma_{2,1}^+) \in p\text{-PCP}[p \cdot m \log m, p \cdot m \log m]$.*

Proof. We can modify the SC function to cope with greater clause length and positive rather than negative literals:

$$SC(A, y) = \sum_{x_1, \dots, x_p \in \mathbb{B}^m} \prod_{i \in \{1, p\}} C_{y,i}(x_i)(1 - A(x_i))$$

The family of functions $C_{c,i}$ is also extended in the obvious way.

Then the protocol continues for $p \cdot m$ rounds rather than the $2 \cdot m$ as for the $\Gamma_{1,2}^-$ case. We then need a factor of p extra random bits, and we require p values of the satisfying assignment A for the final evaluation. \square

Corollary 19. *For every parameterized problem $\Pi \in W[2]$ there exists a function $f : \mathbb{N} \rightarrow \mathbb{N}$ such that $\Pi \in p\text{-PCP}[p \cdot (f(k) + \log n) \log(f(k) + \log n), p \cdot (f(k) + \log n) \log(f(k) + \log n)]$ and hence $W[2] \subseteq p\text{-PCP}[p \cdot (f(k) + \log n) \log(f(k) + \log n), p \cdot (f(k) + \log n) \log(f(k) + \log n)]$ where n is the size of the instance and k is the parameter and p is the length of the longest clause in the equivalent $\text{WSAT}(\Gamma_{2,1}^+)$ instance.*

The catch with this of course is that p may, in principle, be as long as the formula and hence $O(f(k)n^{O(1)})$, in which case we do no better (actually, clearly worse) than the trivial $p\text{-PCP}$ guaranteed by the fact that $W[2] \subseteq \text{para-NP}$.

4.3 Extension to Bounded Parameterized Classes

As $\text{WSAT}(2\text{-CNF}^-)$ is complete for both $\text{EXPW}[1]$ [31] and $\text{EW}[1]$ [23], we can easily adapt the $W[1]$ result. We omit the formal particulars of the restriction on the running time and reduction structures denoting them simply by prepending the bound to the nomenclature.

Corollary 20. *$\text{EXPW}[1] \subseteq 2^{k^{O(1)}}\text{-}p\text{-PCP}[(2^{k^{O(1)}} + \log n) \log(2^{k^{O(1)}} + \log n), (2^{k^{O(1)}} + \log n) \log(2^{k^{O(1)}} + \log n)]$ where n is the size of the instance and k is the parameter.*

Corollary 21. *$\text{EW}[1] \subseteq 2^{O(k)}\text{-}p\text{-PCP}[(2^{O(k)} + \log n) \log(2^{O(k)} + \log n), (2^{O(k)} + \log n) \log(2^{O(k)} + \log n)]$ where n is the size of the instance and k is the parameter.*

As $\text{WSAT}(2\text{-CNF}^-)$ is not $S[1]$ -complete, we need to adjust the formula CS used in Theorem 1 as we can no longer assume that all variables are negated. Fortunately we can simply use the formula of Feige *et al.* [20] more directly (adjusted for 2-CNF, rather than 3-CNF). Recall that $2^m \geq \max\{\text{var}(\phi), \text{cl}(\phi)\}$ (of course we are really just interested in taking a power of two so that the logarithms work neatly). As $\text{var}(\phi) = k'$ is the parameter we know that $m \leq \log(4k'^2)$. Given that k is the parameter of the initial problem and n is the size, the reduction scheme that closes the S -hierarchy gives $k' = g(l)(k + \log n)$ for some $SUBEPT$ -time computable function g over \mathbb{N} .

Corollary 22. $S[1] \subseteq 2^{o^{eff}(k)}\text{-}p\text{-PCP}[\log(g'(l)(k + \log n)^2) \log \log(g'(l)(k + \log n)^2), \log(g'(l)(k + \log n)^2) \log \log(g'(l)(k + \log n)^2)]$ where n is the size of the instance, k is the parameter and g' is a $SUBEPT$ -time computable function over \mathbb{N} .

Then from the miniaturization isomorphism we get:

Corollary 23. $M[1] \subseteq p\text{-PCP}[\log(f(\frac{k}{\log n})n^{O(1)}) \log \log(f(\frac{k}{\log n})n^{O(1)}), \log(f(\frac{k}{\log n})n^{O(1)}) \log \log(f(\frac{k}{\log n})n^{O(1)})]$ where n is the size of the instance and $\frac{k}{\log n}$ is the parameter.

5 Proof Checking for the A -Hierarchy

Looking at the classes of the A -hierarchy, one may be put in mind of Shamir's [30] proof that $\text{IP} = \text{PSPACE}$ via a Lund *et al.* [28] style protocol over instances of the QUANTIFIED BOOLEAN SATISFIABILITY problem. However, the restriction of the weight of the solution poses some interesting problems. While in Shamir's case, the universal quantification is truly universal, in ours it is universal only in the "for all subsets of size k " sense, hence it is difficult to translate an instance of AWSAT in the same fashion — dealing with each universally quantified variable individually becomes complicated by the fact that its possible values depend on how many of the previous variables have been set to TRUE, which is further complicated by the assignment of a random value out of a much larger field.

From the parameterized perspective, it is also perhaps not sensible that we ask to verify a membership proof of an AWSAT problem in FPT-time. If we consider a certificate for such an instance (with the technical consideration that $l \geq 2$) then we must verify not only a single weight k satisfying assignment, but for those variables that are universally quantified, we must verify that *all* weight k_i assignments have accompanying assignments from the existentially quantified variables following them. That is, we are in effect expected to check on the order of n^k assignments. This is reflected in the structure of the parameterized classes — while the W -hierarchy is contained

in *para*-NP, apart from $A[1]$, there is no evidence that the A -hierarchy is. However the A -hierarchy is contained in XP, hence we can solve these problems in time $f(k) + n^{f(k)}$ and naturally can thus check solutions within that bound.

With this in mind we suggest a slightly relaxed version of a parameterized PCP, where we make the obvious changes from FPT-time to $f(k) + n^{f(k)}$. For simplicity we will denote this as a n^k -p-PCP.

Theorem 24. *Let $(\phi, X_1, \dots, X_l, k = k_1 + \dots + k_l)$ be an instance of $\text{AWSAT}_l(\Gamma_{1,2}^-)$ where $\max\{\text{var}(\phi), \text{cl}(\phi)\} \leq 2^m$ with l odd and $k' = k_2 + k_4 + \dots + k_{l-1}$. There is an $(n^{k'} \cdot m \log m, n^{k'} \cdot m \log m)$ -restricted probabilistic $(f(k) + n^{f(k)})$ -time Turing Machine that rejects (ϕ, k) with high probability if $(\phi, X_1, \dots, X_l, k = k_1 + \dots + k_l)$ is a NO-instance of $\text{AWSAT}_l(\Gamma_{1,2}^-)$. That is, $\text{AWSAT}_l(\Gamma_{1,2}^-) \in p\text{-PCP}[n^{k'} \cdot m \log m, n^{k'} \cdot m \log m]$.*

Proof. The verifying TM V begins by generating the $O(n^{k'})$ assignments to the variables of $X_{\text{even}} = X_2 \cup X_4 \cup \dots \cup X_{l-1}$. In effect we can treat this as a simple string s over $\{0, 1\}^{|X_{\text{even}}|}$, which we will use to index elements of the truth assignment given in the proof string (which again we can treat as a table). For each assignment to X_{even} we can reduce the input formula ϕ appropriately in polynomial time, substituting in the values of the literals and simplifying the formula to ϕ' .

We then have a series of $\Gamma_{1,2}^-$ formulæ with only *existential* qualification, but this is equivalent to an instance of $\text{WSAT}(\Gamma_{1,2}^-)$, only with the slight constraint that the truth assignment is required to consist of $\frac{l+1}{2}$ parts, corresponding to the odd indexed variable sets X_1, \dots, X_l .

Thus we can apply the protocol used for $W[1]$, with the slight change that instead of checking simply that $\sum_{x_i} A(x_i) = k$, we check the sequence of truth assignments A_j^s where $j \in \{2h - 1 \mid h \in \mathbb{N}^+\}$, ensuring that for each the weight is k_j . \square

Corollary 25. $A[l] \subseteq p\text{-PCP}[f(k)n^{g(k)} \cdot \log(f(k)n^{O(1)}) \log \log(f(k)n^{O(1)}), f(k)n^{g(k)} \cdot \log(f(k)n^{O(1)}) \log \log(f(k)n^{O(1)})]$ for all $l \geq 1$, where n is the size of the input, k is the parameter and g and f are computable functions.

Proof. As $A[l]$ is closed under fpt-reductions, if l is odd, we can reduce the input instance to an instance of $\text{AWSAT}_l(\Gamma_{1,2}^-)$ with at most $f(k)n^{O(1)}$ clauses and variables, with parameter $g(k)$.

By containment, if l is even, we can reduce the input to an instance of $\text{AWSAT}_{l+1}(\Gamma_{1,2}^-)$. \square

We note particularly that this p -PCP has the nice property of reducing to the $W[1]$ p -PCP in the case where $l = 1$. This is a generally desirable property as $A[1] = W[1]$ (though in general we only expect that $W[t] \subseteq A[t]$).

Corollary 26. $AW[*] \subseteq p\text{-PCP}[f(k)n^{g(k)\cdot\lfloor\frac{l}{2}\rfloor}\cdot\log(f(k)n^{O(1)})\log\log(f(k)n^{O(1)}), f(k)n^{g(k)\cdot\lfloor\frac{l}{2}\rfloor}\cdot\log(f(k)n^{O(1)})\log\log(f(k)n^{O(1)})]$

Proof. Any problem in $AW[*]$ can be reduced to an instance of $AWSAT(\Gamma_{1,2}^-)$. In this case l is not fixed, but part of the input. However for a given instance, the number of even-index variable sets is at most $\lfloor\frac{l}{2}\rfloor$. \square

6 Conclusion

The development of parameterized PCPs, of which this is simply a first step, may have interesting results, particularly for parameterized approximation theory. Currently non-trivial parameterized approximations are few, and the status of key problems such as **CLIQUE** and **DOMINATING SET** are essentially unknown. For parameterized PCPs to have an impact on this however, results need to be improved and extended. By employing directly the construction of Feige *et al.* [20] for **MAX-CLIQUE** we could obtain results if we can reduce the number of random bits of a p -PCP containing $W[1]$ to a function of k alone. This seems possible for the main part of the checking protocol — we can simply randomly generate only k of the values, and take all others as constant (say 0), with a corresponding alteration in the size of the field over which the values are generated, the probability of incorrectly accepting is in essence no different. A similar alteration to the multilinearity testing however is much more difficult. Another possible approach would be to explore the intersection of Dinur’s [17] proof of the PCP theorem which employs certain constraint satisfaction problems and recent hardness results for parameterized versions of constraint satisfaction [11].

Extending the result of this paper to cover other classes also seems to be non-trivial, the alternation of boolean operators of unbounded arity in propositional classes that define the classes $W[t]$ seems to preclude retaining the constant degree property essential to the protocol presented here (this is not a problem for NP as we do not need to keep track of the weight of the satisfying assignment, so the polynomial expansion experienced in reducing a formula to 3-CNF creates no problem). However it seems likely that a tight p -PCP for $W[1]$ would be part of a broader p -PCP that generalizes to $W[t]$ for all t , implying that t will play an important role in the final complexity description.

In the other direction it would be interesting to obtain a more general p -PCP for the other PSPACE related parameterized classes, particularly $AW[SAT]$ and $AW[P]$.

References

- [1] K. A. Abrahamson, R. G. Downey, and M. R. Fellows. Fixed-parameter tractability and completeness IV: On completeness for $W[P]$ and PSPACE analogs. *Annals of Pure and Applied Logic*, 73:235–276, 1995.
- [2] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *Journal of the ACM*, 45(3):501–555, 1998.
- [3] Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs; a new characterization of np. In *33rd Annual Symposium on Foundations of Computer Science, Pittsburgh, Pennsylvania, USA, 24-27 October 1992*, pages 2–13. IEEE Computer Society, 1992.
- [4] Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs: A new characterization of NP. *Journal of the ACM*, 45(1):70–122, 1998.
- [5] László Babai. Trading group theory for randomness. In Robert Sedgewick, editor, *Proceedings of the 17th Annual ACM Symposium on Theory of Computing, May 6-8, 1985, Providence, Rhode Island, USA*, pages 421–429. ACM, 1985.
- [6] László Babai, Lance Fortnow, Leonid A. Levin, and Mario Szegedy. Checking computations in polylogarithmic time. In Cris Koutsougeras and Jeffrey Scott Vitter, editors, *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, May 5-8, 1991, New Orleans, Louisiana, USA*, pages 21–31. ACM, 1991.
- [7] László Babai, Lance Fortnow, and Carsten Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1:3–40, 1991.
- [8] László Babai, Lance Fortnow, and Carsten Lund. Addendum to non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 2:374, 1992.
- [9] László Babai and Shlomo Moran. Arthur-merlin games: A randomized proof system, and a hierarchy of complexity classes. *Journal of Computer and System Sciences*, 36(2):254–276, 1988.
- [10] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Multi-prover interactive proofs: How to remove intractability assumptions. In Janos Simon, editor, *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 113–131. ACM, 1988.

- [11] Andrei A. Bulatov and Dániel Marx. Constraint satisfaction parameterized by solution size. In Luca Aceto, Monika Henzinger, and Jiri Sgall, editors, *Automata, Languages and Programming - 38th International Colloquium, ICALP 2011, Zurich, Switzerland, July 4-8, 2011, Proceedings, Part I*, volume 6755 of *Lecture Notes in Computer Science*, pages 424–436. Springer, 2011.
- [12] Jianer Chen, Benny Chor, Mike Fellows, Xiuzhen Huang, David W. Juedes, Iyad A. Kanj, and Ge Xia. Tight lower bounds for certain parameterized np-hard problems. In *19th Annual IEEE Conference on Computational Complexity (CCC 2004), 21-24 June 2004, Amherst, MA, USA*, pages 150–160. IEEE Computer Society, 2004.
- [13] Jianer Chen, Xiuzhen Huang, Iyad A. Kanj, and Ge Xia. Linear fpt reductions and computational lower bounds. In László Babai, editor, *Proceedings of the 36th Annual ACM Symposium on Theory of Computing, Chicago, IL, USA, June 13-16, 2004*, pages 212–221. ACM, 2004.
- [14] Yijia Chen and Jörg Flum. On miniaturized problems in parameterized complexity theory. In Rodney G. Downey, Michael R. Fellows, and Frank K. H. A. Dehne, editors, *Parameterized and Exact Computation, First International Workshop, IWPEC 2004, Bergen, Norway, September 14-17, 2004, Proceedings*, Lecture Notes in Computer Science, pages 108–120. Springer, 2004.
- [15] Yijia Chen and Martin Grohe. An isomorphism between subexponential and parameterized complexity theory. *SIAM Journal of Computing*, 37(4):1228–1258, 2007.
- [16] Anne Condon. The complexity of the max word problem. In Christian Choffrut and Matthias Jantzen, editors, *STACS 91, 8th Annual Symposium on Theoretical Aspects of Computer Science, Hamburg, Germany, February 14-16, 1991, Proceedings*, volume 480 of *Lecture Notes in Computer Science*, pages 456–465. Springer, 1991.
- [17] Irit Dinur. The PCP theorem by gap amplification. *Journal of the ACM*, 54(3):44, 2007.
- [18] Rodney G. Downey, Vladimir Estivill-Castro, Michael R. Fellows, Elena Prieto, and Frances A. Rosamond. Cutting up is hard to do: the parameterized complexity of k-cut and related problems. *Electronic Notes on Theoretical Computer Science*, 78:209–222, 2003.
- [19] Rodney G. Downey and Michael R. Fellows. *Parameterized Complexity*. Springer, 1999.

- [20] Uriel Feige, Shafi Goldwasser, László Lovász, Shmuel Safra, and Mario Szegedy. Interactive proofs and the hardness of approximating cliques. *Journal of the ACM*, 43(2):268–292, 1996.
- [21] Jörg Flum and Martin Grohe. Parametrized complexity and subexponential time (column: Computational complexity). *Bulletin of the EATCS*, 84:71–100, 2004.
- [22] Jörg Flum and Martin Grohe. *Parameterized complexity theory*. Springer, 2006.
- [23] Jörg Flum, Martin Grohe, and Mark Weyer. Bounded fixed-parameter tractability and $\log^2 n$ nondeterministic bits. *Journal of Computer and System Sciences*, 72(1):34–71, 2006.
- [24] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof-systems (extended abstract). In Robert Sedgewick, editor, *Proceedings of the 17th Annual ACM Symposium on Theory of Computing, May 6-8, 1985, Providence, Rhode Island, USA*, pages 291–304. ACM, 1985.
- [25] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal of Computing*, 18(1):186–208, 1989.
- [26] Shafi Goldwasser and Michael Sipser. Private coins versus public coins in interactive proof systems. In Juris Hartmanis, editor, *Proceedings of the 18th Annual ACM Symposium on Theory of Computing, May 28-30, 1986, Berkeley, California, USA*, pages 59–68. ACM, 1986.
- [27] Russell Impagliazzo, Ramamohan Paturi, and Francis Zane. Which problems have strongly exponential complexity? *Journal of Computer and System Sciences*, 63(4):512–530, 2001.
- [28] Carsten Lund, Lance Fortnow, Howard J. Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, 1992.
- [29] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980.
- [30] Adi Shamir. $IP=PSPACE$. In *31st Annual Symposium on Foundations of Computer Science, St. Louis, Missouri, USA, October 22-24, 1990, Volume I*, pages 11–15. IEEE Computer Society, 1990.
- [31] Mark Weyer. Bounded fixed-parameter tractability: The case $2poly(k)$. In Rodney G. Downey, Michael R. Fellows, and Frank K. H. A. Dehne, editors, *Parameterized and Exact Computation, First International*

Workshop, IWPEC 2004, Bergen, Norway, September 14-17, 2004, Proceedings, volume 3162 of *Lecture Notes in Computer Science*, pages 49–60. Springer, 2004.